

## UNITED STATES DISTRICT COURT

for the  
Western District of Washington

## In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)

Screen/User Name: vahinephoto.com with associated email addresses of  
g.maes@nda.ddec.pf (verified) and tazerty@gmail.com, a phone  
number 689714770, and address: BP 679 Papeete Tahiti 98713 FR,  
more fully described in Attachment A.

Case No. MJ24-173

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Screen/User Name: vahinephoto.com with associated email addresses of g.maes@nda.ddec.pf (verified) and tazerty@gmail.com, a phone number 689714770, and address: BP 679 Papeete Tahiti 98713 FR, more fully described in Attachment A.

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

## Code Section

18 U.S.C. § 2252(a)(4)(B), (b)(2)  
 18 U.S.C. § 2252(a)(1), (b)(1)

## Offense Description

Possession of Child Pornography  
 Transportation of Child Pornography

The application is based on these facts:

- ☒ See Affidavit of Special Agent Shafqat M. Mirza, continued on the attached sheet.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.

SHAFQAT M MIRZA

Digitally signed by SHAFQAT M

MIRZA

Date: 2024.03.19 09:58:26 -07'00'

Applicant's signature

Shafqat M. Mirza, Special Agent (HSI)

Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or  
☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 03/20/2024



Judge's signature

City and state: Seattle, Washington

Michelle L. Peterson, United States Magistrate Judge

Printed name and title

STATE OF WASHINGTON           )  
   )          ss  
COUNTY OF KING               )

I, Shafqat M. Mirza, a Special Agent with Homeland Security Investigations (HSI) in Seattle, Washington, having been first duly sworn, hereby depose and state as follows:

1. I make this affidavit in support of an application for a search warrant for information associated with a certain Adobe Systems Incorporated account that is stored at premises owned, maintained, controlled, or operated by Adobe Systems Incorporated (“Adobe”), a company headquartered in San Francisco, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Adobe Systems Incorporated to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the account.

2. I am a Special Agent (“SA”) with the Department of Homeland Security (“DHS”), U.S. Immigration and Customs Enforcement (“ICE”), Homeland Security Investigations (“HSI”). I have held such a position since December 2021. HSI is responsible for enforcing the customs and immigration laws and federal criminal statutes of the United States. I am currently assigned to the Office of the Special Agent in Charge (“SAC”), Seattle, Washington, and am a member of the Child Exploitation Investigations Group. As part of my current duties, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal

1 production, distribution, receipt, and possession of child pornography and material  
2 involving the sexual exploitation of minors in violation of 18 U.S.C. §§ 2251, 2252, and  
3 2252A. I have also had the opportunity to observe and review examples of child  
4 pornography (as defined in 18 U.S.C. § 2256(8)).

5 3. As part of my current duties as an HSI Criminal Investigator, I investigate  
6 criminal violations relating to child exploitation and child pornography including  
7 violations of Title 18, United States Code, Sections 2251(a), 2252(a)(2), 2252(a)(4)(B),  
8 and 2243(a)(1). I have received training about child pornography and child exploitation,  
9 and have observed and reviewed numerous examples of child pornography in various  
10 forms of media, including media stored on digital media storage devices such as  
11 computers, tablets, cellphones, etc. I am a graduate of the Criminal Investigator Training  
12 Program (“CITP”), and the HSI Special Agent Training (“HSISAT”) at the Federal Law  
13 Enforcement Training Center in Glynco, Georgia. I have participated in the execution of  
14 previous search warrants, which involved child exploitation and/or child pornography  
15 offenses, and the search and seizure of computers, related peripherals, and computer  
16 media equipment. I am a member of the Seattle Internet Crimes Against Children Task  
17 Force (“ICAC”), and work with other federal, state, and local law enforcement personnel  
18 in the investigation and prosecution of crimes involving the sexual exploitation of  
19 children.

20 4. The facts in this affidavit come from my personal observations, my training  
21 and experience, and information obtained from other agents and witnesses. This affidavit  
22 is intended to show merely that there is sufficient probable cause for the requested  
23 warrants and does not set forth all of my knowledge about this matter.

24 Based on my training and experience and the facts as set forth in this affidavit, there is  
25 probable cause to believe that violations of Title 18, U.S.C., § 2252(a)(4)(B), (b)(2),  
26 Possession of Child Pornography, and Transportation of Child Pornography Title 18,  
27 U.S.C. 2252(a)(1), (b)(1), has been committed by Gabriel Maes. There is also probable

1 cause to search the information described in Attachment A, specifically: **Username:**  
 2 **vahinephoto.com** for evidence of these crimes and contraband or fruits of these crimes,  
 3 as described in Attachment B.

#### 4 DEFINITIONS

5 The following definitions apply to this affidavit:

6 5. “Chat,” as used herein, refers to any kind of text communication over the  
 7 internet that is transmitted in real-time from sender to receiver. Chat messages are  
 8 generally short in order to enable other participants to respond quickly and in a format  
 9 that resembles an oral conversation. This feature distinguishes chatting from other text-  
 10 based online communications such as internet forums and email.

11 6. “Child erotica,” as used herein, means materials or items that are sexually  
 12 arousing to persons having a sexual interest in children but that are not necessarily  
 13 obscene or do not necessarily depict minors in sexually explicit poses or positions.

14 7. For the purposes of this affidavit, a “minor” refers to any person less than  
 15 eighteen years of age and for the purpose of this search warrant, “Child pornography,” as  
 16 used herein, is defined in 18 U.S.C. § 2256 (any visual depiction of sexually explicit  
 17 conduct where (a) the production of the visual depiction involved the use of a minor  
 18 engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer  
 19 image, or computer-generated image that is, or is indistinguishable from, that of a minor  
 20 engaged in sexually explicit conduct, or (c) the visual depiction has been created,  
 21 adapted, or modified to appear that an identifiable minor is engaged in sexually explicit  
 22 conduct).

23 8. “Sexually explicit conduct” means actual or simulated (a) sexual  
 24 intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons  
 25 of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic  
 26 abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18  
 27 U.S.C. § 2256(2).

1           9.     “Cloud-based storage service,” as used herein, refers to a publicly  
2 accessible, online storage provider that collectors of depictions of minors engaged in  
3 sexually explicit conduct can use to store and trade depictions of minors engaged in  
4 sexually explicit conduct in larger volumes. Users of such a service can share links and  
5 associated passwords to their stored files with other traders or collectors of depictions of  
6 minors engaged in sexually explicit conduct in order to grant access to their collections.  
7 Such services allow individuals to easily access these files through a wide variety of  
8 electronic devices such as desktop and laptop computers, mobile phones, and tablets,  
9 anywhere and at any time. An individual with the password to a file stored on a cloud-  
10 based service does not need to be a user of the service to access the file. Access is free  
11 and readily available to anyone who has an internet connection.

12           10.    “Computer,” as used herein, refers to “an electronic, magnetic, optical,  
13 electrochemical, or other high speed data processing device performing logical or storage  
14 functions, and includes any data storage facility or communications facility directly  
15 related to or operating in conjunction with such device,” including smartphones and  
16 mobile devices.

17           11.    “Data,” as used herein refers to the quantities, characters, or symbols on  
18 which operations are performed by a computer, being stored and transmitted in the form  
19 of electrical signals and recorded on magnetic, optical, or mechanical recording media.

20           12.    “Digital Devices” as used herein refers to any physical object that has a  
21 computer, microcomputer, or hardware that is capable of receiving, storing, possessing,  
22 or potentially sending data.

23           13.    “File Transfer Protocol” (“FTP”), as used herein, is a standard network  
24 protocol used to transfer computer files from one host to another over a computer  
25 network, such as the internet. FTP is built on client-server architecture and uses separate  
26 control and data connections between the client and the server.

14. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations, community-owned, non-profit, or otherwise privately-owned companies that are in business to provide individuals and businesses access to the internet. ISPs provide a range of functions for their customers including access to the internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

15. “Mobile applications,” as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

16. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

17. “User Attributes,” as used herein refers to any tangible data, documents, settings, programs, or other information that provides information related to the identity of the specific user of the device, computer, application, program, or record.

## BACKGROUND

Based on my training, experience and collaboration with agents and detectives investigating child exploitation, industry experts, academia and other law enforcement personnel, I know the following:

18. That adult persons with a sexual interest in minors are persons whose sexual targets are children. They receive sexual gratification and satisfaction from actual physical contact with children, fantasy involving the use of writings detailing physical contact with children, and/or from fantasy involving the use of pictures and/or videos of minors.

19. The development of the computer has changed the way children are engaged in sexually explicit conduct and the files created therefrom are distributed thereafter. The computer serves four functions in connection with depictions of children

1 engaged in sexually explicit conduct. These four functions include: production,  
2 communications, distribution, and storage.

3 20. Pornographers produce both still and moving images, i.e.: photographs and  
4 video. These files can be transferred either directly from the camera/camera phone into a  
5 computer or mobile application, directly from a storage device such as a flash drive to a  
6 computer, or the image files can be transferred directly into the computer by use of a  
7 scanner.

8 21. In addition to data sharing between phones, mobile and desktop  
9 applications, and websites, e-mail may also be used electronically transmits files through  
10 a user's electronic device.

11 22. All that a smart phone or computer user needs to do in order to use an  
12 application, website, or email is open up an account with one of the myriad of companies  
13 that provide services (e.g. Meta, Microsoft, Google, Discord, Dropbox, etc.). Once the  
14 account is set up, the user can choose the "name" of his/her account, which does not have  
15 to match (or even relate to) identifying information of the user. Thus, the user name by  
16 itself does nothing to identify the owner of the account, the user, or the composer of the  
17 communication. Nevertheless, often times the communications themselves, contain  
18 information that either directly or indirectly identifies the composer of the file. Based on  
19 my training and experience investigating child exploitation offenses, I know it is common  
20 for collectors of depictions of minors engaged in sexually explicit conduct to use multiple  
21 social media accounts and/or applications in order conceal their true identity and/or more  
22 easily categorize their collection according to the type of material or source.

23 23. Individuals involved in computer-related crimes often use these accounts to  
24 conduct both criminal and non-criminal communications. Consequently, these  
25 communications can be a great source of information to help identify the sender and/or  
26 recipient of the file and/or message. The ability to view these communications by  
27

1 investigating law enforcement often provides further investigative leads to assist in  
2 identifying the person of interest.

3       24. I know that an Internet Protocol (IP) address is a numerical label assigned  
4 to devices communicating on the internet and that the Internet Assigned Numbers  
5 Authority (IANA) manages the IP address space allocations globally. An IP address  
6 provides the methodology for communication between devices on the internet. It is a  
7 number that uniquely identifies a device on a computer network and, using transport  
8 protocols, moves information on the internet. Every device directly connected to the  
9 internet must have a unique IP address.

10       25. An IP address is typically comprised of four (4) series of numbers separated  
11 by periods and is most commonly represented as a 32-bit number such as 71.227.252.216  
12 (Internet Protocol Version 4). IPv6 is deployed as well and is represented as a 128-bit  
13 number such as 2001:db8:0:1234:0:567:8:1.

14       26. IP addresses are owned by the Internet Service Provider and leased to a  
15 subscriber/customer for a period of time. They are public and visible to others as you  
16 surf the internet. The lessee has no expectation of privacy due to the public nature of IP  
17 addresses.

18       27. When an Internet Service Provider's customer logs onto the internet using a  
19 computer or another web-enabled device, they are assigned an Internet Protocol (IP)  
20 address.

21       28. There are two different types of Internet Protocol addresses. The first is a  
22 dynamic IP address, which means the user's IP address may change each time they log on  
23 to the internet. The frequency in which this address changes is generally controlled by  
24 the Internet Service Provider and not the user. The other type of IP address is a static IP  
25 address, which means that a user is assigned a specific IP address that remains constant  
26 every time they log on to the internet.  
27

1           29. IP addresses are similar to a license plate on a motor vehicle. They are the  
2 property of the issuer, and not the vehicle owner. Just as your license plate is visible as  
3 you cruise your city or town, your IP address is visible as you cruise the internet. Your  
4 IP address is visible to the administrators of websites you visit, attached emails you send,  
5 and broadcast during most internet file and information exchanges that occur on the  
6 internet.

7           30. I know based on my training and experience, that Electronic Service  
8 Providers (“ESP”) and/or Internet Service Providers (“ISP,” collectively ISP) typically  
9 monitor their services utilized by subscribers. To prevent their communication networks  
10 from serving as conduits for illicit activity and pursuant to the terms of user agreements,  
11 ISPs routinely and systematically attempt to identify suspected depictions of minors  
12 engaged in sexually explicit conduct that may be sent through its facilities. Commonly,  
13 customer complaints alert them that an image or video file being transmitted through  
14 their facilities likely contains suspected depictions of minors engaged in sexually explicit  
15 conduct.

16           31. When an ESP/ISP receives such a complaint or other notice of suspected  
17 depictions of minors engaged in sexually explicit conduct, they may employ a “graphic  
18 review analyst” or an equivalent employee to open and look at the image or video file to  
19 form an opinion as to whether what is depicted likely meets the federal criminal  
20 definition of depictions of minors engaged in sexually explicit conduct found in 18 USC  
21 § 2256, which is defined as any visual depiction, including any photograph, film, video,  
22 picture, or computer or computer-generated image or picture, whether made or produced  
23 by electronic, mechanical, or other means, of sexually explicit conduct, where: (A) the  
24 production of such visual depiction involves the use of a minor engaging in sexually  
25 explicit conduct; (B) such visual depiction is a digital image, computer image, or  
26 computer-generated image that is, or is indistinguishable from, that of a minor engaging  
27 in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or

1 modified to appear that an identifiable minor is engaging in sexually explicit conduct. If  
2 the employee concludes that the file contains what appears to be depictions of minors  
3 engaged in sexually explicit conduct, a hash value of the file can be generated by  
4 operation of a mathematical algorithm. A hash value is an alphanumeric sequence that is  
5 unique to a specific digital file. Any identical copy of the file will have exactly the same  
6 hash value as the original, but any alteration of the file, including even a change of one or  
7 two pixels, results in a different hash value. Consequently, an unknown image can be  
8 determined to be identical to an original file if it has the same hash value as the original.  
9 The hash value is, in essence, the unique fingerprint of that file, and when a match of the  
10 “fingerprint” occurs, the file also matches. Several different algorithms are commonly  
11 used to hash-identify files, including Message Digest 5 (MD5) and Secure Hash  
12 Algorithm 1 (SHA-1).

13 32. Hash values are a very reliable method of authenticating files. It can be  
14 concluded with an extremely high degree of certainty that two files sharing the same hash  
15 value also share identical content. Based on my training and experience, as well as others  
16 in this field, I know it is more likely that two humans would share the same biological  
17 DNA than for two files to share the same hash value. If even one bit (the smallest  
18 measure of data in a file) of a file is changed, the entire hash value of that file changes  
19 completely. As an example that demonstrates the uniqueness of a SHA-1 hash, the  
20 likelihood of two files having the same SHA-1 hash value is  $2^{128}$  or:1 in  
21 340,000,000,000,000,000,000,000,000,000,000,000,000,000,000 chance. In an August 6<sup>th</sup>, 2020  
22 article in Live Science<sup>1</sup>, according to Professor Simona Francese, PhD, a forensic  
23 scientist and fingerprint expert from Sheffield Hallam University in the United Kingdom,

24  
25  
26  
27 <sup>1</sup> Baker, Harry. “Do Identical Twins Have Identical Fingerprints?” LiveScience, Purch, 7 Aug. 2021,  
<https://www.livescience.com/do-identical-twins-have-identical-fingerprints.html>.

1 the likelihood of two humans having the same fingerprint is estimated to be:1 in  
2 64,000,000,000.<sup>2</sup>

3 33. For two different files to have the same hash value is called a *collision*. I  
4 know from experience that there have been no documented incidents of a collision  
5 involving SHA-1 hash values “in the wild” since its creation in 1995. I am, however,  
6 aware of a reported collision involving two files sharing the same SHA-1 value in a lab  
7 setting. This was done purposely by engineers at Google<sup>3</sup> in 2017 under controlled  
8 conditions for the sole purpose of creating this collision. Even with this knowledge in  
9 mind, I am confident that the possibility of a suspected child sexual abuse material file  
10 reported in a CyberTip having the same hash value as an unrelated, non-criminal file is  
11 extremely unlikely. I believe hash value comparison is a highly reliable method of  
12 determining if two files are the same or different, and that a confirmed hash match  
13 between two files is a forensic finding on a par with a DNA match or a fingerprint match.

14 34. ESPs typically maintain a database of hash values of files that they have  
15 determined to meet the federal definition of depictions of minors engaged in sexually  
16 explicit conduct found in 18 USC § 2256. The ISPs typically do not maintain the actual  
17 suspect files themselves; once a file is determined to contain suspected depictions of  
18 minors engaged in sexually explicit conduct, the file is deleted from their system.

19 35. The ESPs can then use Image Detection and Filtering Process (“IDFP”),  
20 Photo DNA (pDNA), or a similar technology which compares the hash values of files  
21 embedded in or attached to transmitted files against their database containing what is  
22 essentially a catalog of hash values of files that have previously been identified as  
23 containing suspected depictions of minors engaged in sexually explicit conduct.

---

25 <sup>2</sup> Of note, in the same article, Professor Francese, who is a peer-reviewed, published scientist, commented, “to this  
26 day, no two fingerprints have been found to be identical.”

27 <sup>3</sup> “Announcing the First sha1 Collision.” *Google Online Security Blog*, 23 Feb. 2017,  
<https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html>.

1           36. When the ESP detects a file passing through its network that has the same  
2 hash value as an image or video file of suspected depictions of minors engaged in  
3 sexually explicit conduct contained in the database through a variety of methods, the ISP  
4 reports that fact to National Center for Missing and Exploited Children (NCMEC) via the  
5 latter's CyberTipline. By statute, an ESP or ISP has a duty to report to NCMEC any  
6 apparent depictions of minors engaged in sexually explicit conduct it discovers "as soon  
7 as reasonably possible." 18 U.S.C. § 2258A(a)(1). The CyberTip line report transmits  
8 the intercepted file to NCMEC. Often that occurs without an ISP employee opening or  
9 viewing the file because the files hash value, or "fingerprint," has already been associated  
10 to a file of suspected depictions of minors engaged in sexually explicit conduct. The  
11 ISP's decision to report a file to NCMEC is made solely on the basis of the match of the  
12 unique hash value of the suspected depictions of minors engaged in sexually explicit  
13 conduct to the identical hash value in the suspect transmission.

14           37. ESP's also monitor which devices are used to access their platform by  
15 recording the advertising identification number. This number is a unique identifier  
16 assigned to hardware devices used by ESP's to track users semi-anonymously and  
17 provide targeted advertisements. Because it is a unique identifier, this information can  
18 link specific devices owned by specific individuals with the criminal activity on a  
19 particular platform's account.

20           38. Most Internet Service Providers keep subscriber records relating to the IP  
21 address they assign, and that information is available to investigators. Typically, an  
22 investigator has to submit legal process (e.g. subpoena or search warrant) requesting the  
23 subscriber information relating to a particular IP address at a specific date and time.

24           39. A variety of publicly available websites provide a public query/response  
25 protocol that is widely used for querying databases in order to determine the registrant or  
26 assignee of internet resources, such as a domain name or an IP address block. These  
27 include WHOIS, MaxMind, arin.net, and other common search tools.

1           40. The act of “downloading” is commonly described in computer networks as  
2 a means to receive data to a local system from a remote system, or to initiate such a data  
3 transfer. Examples of a remote system from which a download might be performed  
4 include a webserver, FTP server, email server, or other similar systems. A download can  
5 mean either any file that is offered for downloading or that has been downloaded, or the  
6 process of receiving such a file. The inverse operation, “uploading,” refers to the sending  
7 of data from a local system to a remote system such as a server or another client with the  
8 intent that the remote system should store a copy of the data being transferred, or the  
9 initiation of such a process.

10           41. The National Center for Missing and Exploited Children (NCMEC) is a  
11 private, non-profit organization established in 1984 by the United States Congress.  
12 Primarily funded by the Justice Department, the NCMEC acts as an information  
13 clearinghouse and resource for parents, children, law enforcement agencies, schools, and  
14 communities to assist in locating missing children and to raise public awareness about  
15 ways to prevent child abduction, child sexual abuse and depictions of minors engaged in  
16 sexually explicit conduct.

17           42. The Center provides information to help locate children reported missing  
18 (by parental abduction, child abduction, or running away from home) and to assist  
19 physically and sexually abused children. In this resource capacity, the NCMEC  
20 distributes photographs of missing children and accepts tips and information from the  
21 public. It also coordinates these activities with numerous state and federal law  
22 enforcement agencies.

23           43. The CyberTipline offers a means of reporting incidents of child sexual  
24 exploitation including the possession, manufacture, and/or distribution of depictions of  
25 minors engaged in sexually explicit conduct; online enticement; child prostitution; child  
26 sex tourism; extra familial child sexual molestation; unsolicited obscene material sent to a  
27 child; and misleading domain names, words, or digital images.

1           44. Any incidents reported to the CyberTipline online or by telephone go  
2 through this three-step process: CyberTipline operators review and prioritize each lead;  
3 NCMEC's Exploited Children Division analyzes tips and conducts additional research;  
4 The information is accessible to the FBI, ICE, and the USPIS via a secure Web  
5 connection. Information is also forwarded to the ICACs and pertinent international, state,  
6 and local authorities and, when appropriate, to the ESP.

7           45. Based upon my knowledge, experience, and training in depictions of  
8 minors engaged in sexually explicit conduct investigations, and the training and  
9 experience of other law enforcement officers with whom I have had discussions, I know  
10 that there are certain characteristics common to individuals involved in depictions of  
11 minors engaged in sexually explicit conduct:

12           a. Those who possess, receive, and attempt to receive depictions of  
13 minors engaged in sexually explicit conduct may receive sexual gratification, stimulation,  
14 and satisfaction from contact with children; or from fantasies they may have viewing  
15 children engaged in sexual activity or in sexually suggestive poses, such as in person, in  
16 photographs, or other visual media; or from literature describing such activity.

17           b. Those who possess, receive, and attempt to receive depictions of  
18 minors engaged in sexually explicit conduct may collect sexually explicit or suggestive  
19 materials in a variety of media, including photographs, magazines, motion pictures,  
20 videotapes, books, slides, and/or drawings or other visual media. Such individuals often  
21 times use these materials for their own sexual arousal and gratification. Further, they  
22 may use these materials to lower the inhibitions of children they are attempting to seduce,  
23 to arouse the selected child partner, or to demonstrate the desired sexual acts. These  
24 individuals may keep records, to include names, contact information, and/or dates of  
25 these interactions, of the children they have attempted to seduce, arouse, or with whom  
26 they have engaged in the desired sexual acts.

27           c. Those who possess, receive, and attempt to receive depictions of  
minors engaged in sexually explicit conduct often possess and maintain their "hard  
copies" of child pornographic material, that is, their pictures, films, video tapes,  
magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings,  
etc., in the privacy and security of their home or some other secure location. These  
individuals typically retain these "hard copies" of child pornographic material for many  
years.

1 d. Likewise, those who possess, receive, and attempt to receive  
2 depictions of minors engaged in sexually explicit conduct often maintain their collections  
3 that are in a digital or electronic format in a safe, secure and private environment, such as  
4 a computer and surrounding area. These collections are often maintained for several  
5 years and are kept close by, usually at the individual's residence, to enable the collector  
6 to view the collection, which is valued highly.

7 e. Those who possess, receive, and attempt to receive depictions of  
8 minors engaged in sexually explicit conduct also may correspond with and/or meet others  
9 to share information and materials; rarely destroy correspondence from other depictions  
10 of minors engaged in sexually explicit conduct distributors/collectors; conceal such  
11 correspondence as they do their sexually explicit material; and often maintain lists of  
12 names, addresses, and telephone numbers of individuals with whom they have been in  
13 contact and who share the same interests in depictions of minors engaged in sexually  
14 explicit conduct.

15 f. Those that possess, receive and attempt to receive depictions of  
16 minors engaged in sexually explicit conduct prefer not to be without their depictions of  
17 minors engaged in sexually explicit conduct for any prolonged time period. This  
18 behavior has been documented by law enforcement officers involved in the investigation  
19 of depictions of minors engaged in sexually explicit conduct throughout the world.

20 46. Based on my training and experience, collectors and distributors of  
21 depictions of minors engaged in sexually explicit conduct also use online, remote,  
22 resources to retrieve and store depictions of minors engaged in sexually explicit conduct,  
23 including services offered by many companies for cloud-storage and digital  
24 communications. The online services allow a user to set up an account with a remote  
25 computing service that provides email services and/or electronic storage of electronic  
26 files in any variety of formats. A user can set up, and access, an online storage account  
27 from any computer or digital device with access to the internet. Evidence of such online  
storage of depictions of minors engaged in sexually explicit conduct is often found on the  
user's computer or smart phone. Even in cases where online storage is used, however,  
evidence of depictions of minors engaged in sexually explicit conduct can be found on a  
user's digital device if that device is used to access the internet. Cloud storage allows the  
offender ready access to the material from any device that has an internet connection,

1 worldwide, while also attempting to obfuscate or limit the criminality of possession as the  
2 material is stored remotely and not on the offender's device. Evidence located in cloud  
3 storage may be deleted from any device capable of reaching the website of the cloud  
4 hosting company. Once the individual user credentials, often a username and password  
5 are entered, the data in the cloud storage may be accessed, modified, shared, or deleted.  
6 Unlike deleting data from a local hard drive, once data is deleted from cloud storage, it is  
7 wiped from the cloud hosting company's servers and is unrecoverable.

8 47. In addition to the traditional collector, law enforcement has encountered  
9 offenders who obtain depictions of minors engaged in sexually explicit conduct from the  
10 internet, view the contents and subsequently delete the contraband, often after engaging  
11 in self-gratification. In light of technological advancements, increasing internet speeds  
12 and worldwide availability of child sexual exploitative material, this phenomenon offers  
13 the offender a sense of decreasing risk of being identified and/or apprehended with  
14 quantities of contraband. This type of consumer is commonly referred to as a 'seek and  
15 delete' offender, knowing that the same or different contraband satisfying their interests  
16 remain easily discoverable and accessible online for future viewing and self-gratification.

17 48. Additionally, offenders may opt to store the contraband in cloud accounts.  
18 Cloud storage is a model of data storage where the digital data is stored in logical pools,  
19 the physical storage can span multiple servers, and often locations, and the physical  
20 environment is typically owned and managed by a hosting company. Cloud storage  
21 allows the offender ready access to the material from any device that has an internet  
22 connection, worldwide, while also attempting to obfuscate or limit the criminality of  
23 possession as the material is stored remotely and not on the offender's device.

24 49. Based on my training and experience and my consultation with computer  
25 forensic detectives and agents who are familiar with searches of computers and  
26 smartphones, I have learned that offenders will try and obfuscate data containing images  
27 and videos of minors engaged in sexual activity. One potential manner of trying to hide

1 the contraband may be by changing file extensions. For example, an image file may often  
2 have a file extension of “.jpg” or “.jpeg” signifying that it is an image or photograph. An  
3 offender may change the file extension by selecting the “save as” format on a computer  
4 or digital device and select “.doc” or “.docx” to make it appear that instead of a  
5 contraband image or photograph, it is a word document. The same process may be used  
6 to attempt to hide a video file as well. Based on these, and other attempts to hide potential  
7 contraband is necessary for forensic examiners to examine all potential data on a digital  
8 device.

9 50. I know that, regardless of whether a person discards or collects depictions  
10 of minors engaged in sexually explicit conduct he accesses for purposes of viewing and  
11 sexual gratification, evidence of such activity is likely to be found on computers and  
12 related devices, including storage media, used by the person. This evidence may include  
13 the files themselves, logs of account access events, contact lists of others engaged in  
14 trafficking of depictions of minors engaged in sexually explicit conduct, backup files, and  
15 other electronic artifacts that may be forensically recoverable.

16 **BACKGROUND CONCERNING ADOBE SYSTEMS INCORPORATED**<sup>4</sup>

17 51. From research and experience, I know that the company Adobe refers to an  
18 American multi-national computer software company. Adobe provides a variety of on-  
19 line services and software including, most notably, Adobe Photoshop. These tools can be  
20 accessed via Adobe’s website. Adobe allows subscribers to obtain accounts at the  
21 domain name www.adobe.com. Subscribers obtain an Adobe account by registering with  
22 an email address. During the registration process, Adobe asks subscribers to provide  
23 basic personal identifying information. This information can include the subscriber’s full  
24 name, birthdate, e-mail address and other identifiers, alternative e-mail addresses, and,  
25

26 <sup>4</sup> The information in this section is based on information published by Adobe’s Law Enforcement Guidelines  
27 including, but not limited to, the following webpage: <https://www.adobe.com/trust/transparency/law-enforcement-guidelines.html>.

1 for paying subscribers, means and source of payment (including any credit or bank  
2 account number).

3 52. When the subscriber transfers a file to an Adobe account, it is initiated at  
4 the user's computer, transferred via the internet to the Adobe servers, and then can be  
5 edited or manipulated using Adobe's software. If the subscriber does not delete the  
6 content, the files can remain on Adobe's servers indefinitely.

7 53. Online storage providers typically retain certain transactional information  
8 about the creation and use of each account on their systems. This information can  
9 include the date on which the account was created, the length of service, records of log-in  
10 (i.e., session) times and durations, the types of service utilized, the status of the account  
11 (including whether the account is inactive or closed), the methods used to connect to the  
12 account, and other log files that reflect usage of the account. In addition, online storage  
13 providers often have records of the Internet Protocol address ("IP address") used to  
14 register the account and the IP addresses associated with particular logins to the account.  
15 Because every device that connects to the internet must use an IP address, IP address  
16 information can help to identify which computers or other devices were used to access  
17 the account.

18 54. In some cases, Adobe account users will communicate directly with Adobe  
19 about issues relating to the account, such as technical problems, billing inquiries, or  
20 complaints from other users. Online storage providers typically retain records about such  
21 communications, including records of contacts between the user and the provider's  
22 support services, as well records of any actions done by the provider or user as a result of  
23 the communications.

#### 24 **SUMMARY OF PROBABLE CAUSE**

25 **A. CR24-033 TL: Transportation of Child Pornography Title 18, United States**  
26 **Code Sections 2252(a)(1), (b)(1).**

1           55. On July 19, 2023, Homeland Security Investigations (HSI) Seattle received  
2 information from Customs Border Protection (CBP) officers at Seattle Tacoma  
3 International Airport that Gabriel MAES (DOB 1985) arrived on a flight in bound from  
4 Paris, France to Seattle on Air Tahiti Nui (TN 57) with the final destination of Tahiti.  
5 MAES was selected for a secondary examination during which MAES consented to the  
6 search of his electronic devices.

7           56. After MAES was encountered in secondary inspection, it was discovered  
8 that MAES was in possession of ten electronic devices to include one Apple iPhone 12  
9 Pro, one Apple iPad Pro, one Macbook Pro, six hard drives, and an Apple watch. MAES  
10 stated that all electronic devices in his possession belonged to him. MAES gave consent  
11 to HSI to manually review his electronic devices and provided passcodes to access to the  
12 iPhone 12 Pro, iPad Pro, and Macbook Pro. I know from training and experience, that  
13 none of the above listed devices are manufactured in the State of Washington.

14           57. During HSI's manual review of MAES' devices, child sexual abuse  
15 material (CSAM) was discovered. Based on the information obtained, MAES was  
16 detained and interviewed.

17           58. Shortly thereafter, HSI Seattle agents SA Dussler and I arrived at the  
18 Seattle-Tacoma International Airport and conducted a manual review of MAES' devices.  
19 MAES' Telegram account showed several group chats that appear to indicate  
20 pornographic content involving minors through titles or post descriptions such as "12-16"  
21 or an emoji showing "18" with a prohibited symbol over the number. Two group chats  
22 were discovered on MAES' Telegram account on MAES' iPhone 12 Pro and iPad Pro.  
23 CSAM was discovered on both of those devices within the Telegram application. The  
24 CSAM discovered appears to involve the sexual penetration of minors and bondage.

25           59. During the same manual review, SA Dussler reviewed one video from the  
26 iPad Pro and one video from the iPhone 12 Pro as further described below:  
27

1 a. iPad Pro: one video file was located in the Telegram application in a  
 2 group titled "Secret channel (two heart emoji) (18 prohibited symbol)" and was posted by  
 3 a user on or about August 20, 2021. The video file depicts a prepubescent female that is  
 4 nude from the waist down. The prepubescent female is estimated to be approximately 8  
 5 years old due to the size of the child, lack of hip development, and lack of pubic hair. The  
 6 child is shown lying on her back with a pink sex toy inserted in the child's vagina. The  
 7 child's legs are spread apart to expose her vagina and her knees are bent to show pink  
 8 leather restraints around the child's ankles that are attached to similar pink restraints on  
 9 the child's wrists. The child appears to be wearing a white top and gray knee-height  
 10 socks. The focus of the video is on the child's pubic area and the child's face and torso  
 11 are not shown. The video is approximately 5 minutes and 24 seconds in duration.

12 b. iPhone 12 Pro: one video file, located in the Telegram application in  
 13 a group titled "Nude Party (heart eyes emoji)" was posted by a user on or about  
 14 November 5, 2022, depicts a pubescent female child. The child is estimated to be  
 15 approximately 4 years old due to her overall size and small stature, lack of breast or hip  
 16 development, and lack of pubic hair. The video depicts the child standing in front of a  
 17 nude adult male with his erect penis exposed. The child is wearing a pink sleeveless shirt  
 18 and is performing oral sex on the adult male's penis. Another clip within the video shows  
 19 the child lying on her back wearing the same shirt, nude from the waist down to expose  
 20 her vagina. An adult male is seen performing oral sex on the child's vagina. The adult  
 21 male then attempts to insert his erect penis into the child's vagina, and the child is seen  
 22 pushing the male slightly away with her feet to avoid vaginal penetration. The video is  
 23 approximately 13 minutes and 56 seconds in duration.

24 I have viewed these files and based on my training and experience, I believe the files  
 25 described above meet the federal definition of child pornography, as defined in 18 U.S.C.  
 26 2256(8).

27 60. HSI SA Dussler and I conducted a border search interview of MAES with  
 the assistance of CBP Officer Nicolescu for French translation. CBP Officer Nicolescu  
 stated that she was DHS certified in the French language. MAES was advised of his  
 Miranda rights in both English and French after which he invoked his Miranda rights.  
 Prior to MAES' invocation, he reported that he was employed as a technology teacher at  
 a middle school in Tahiti. HSI Seattle's investigation located a website,  
[www.gabrielmaes.com](http://www.gabrielmaes.com), in which MAES was identified as a photographer and a  
 technology teacher at Le Collège, La Mennais, a private Roman Catholic mixed

1 secondary school in Papeete, Tahiti. The school's website indicated it was currently  
2 serving students in Grades 3 to 6 and that its middle and high school student body was  
3 2,280 students. Following the conclusion of MAES' interview, a total of ten devices were  
4 seized from MAES and transported to the HSI Seattle office.

5 61. On November 21, 2023, HSI I obtained a search warrant from King County  
6 Superior Court to examine MAES' ten devices for evidence of child sexual exploitation  
7 material. A subsequent forensic examination of MAES' iPhone and iPad revealed the  
8 discovery of 223 CSAM image and video files. The following are descriptions of two  
9 such files located on MAES' devices as described below:

10 a. Apple iPhone: An image file depicting a prepubescent female who is  
11 nude from the waist down. The prepubescent female is estimated to be approximately 4-5  
12 years old, due to the size of the child lower body, lack of fat or muscle development, very  
13 small vaginal structure, lack of hair follicles and pubic hair, extremely small and  
14 underdeveloped buttocks and hips. The child is seen lying on her back with both of her  
15 legs spread apart and raised high, while the adult male is attempting to penetrate the  
16 child's vagina with his erect penis. The adult male is seen holding his erect penis in his  
17 left hand and is attempting to force penetrate the child's vagina. The focus of the image is  
18 on the child's pubic area and the adult male's erect penis. No faces are depicted in the  
19 file.

20 b. Apple iPad: An image file of a prepubescent female is depicted  
21 completely nude performing oral sex on an adult male's erect penis. The prepubescent  
22 female is estimated to be approximately 3-5 years old, due to the small size of the child's  
23 body compared to the adult male's body, lack of fat or muscle development of the child's  
24 hands, arms, and shoulders. The child is seen partially lying on top of the adult male who  
25 is nude from waist down. The child's face is right above the adult male's erect penis  
26 while she is seen holding the adult male's penis with her hands. Semen can be seen  
27 dripping from the child's lips and from her hand, depicting completion of oral sex after  
the adult male had ejaculated. The focus of the image is on the child's face and the adult  
male's penis.

62. I have viewed these files and based on my training and experience, I  
believe the files described above meet the federal definition of child pornography, as  
defined in 18 U.S.C. 2256(8).

63. On February 14, 2024, a grand jury sitting in the Western District of Washington issued an indictment charging MAES with one count of Transportation of Child Pornography in violation of Title 18, United States Code, Sections 2252(a)(1),(b)(1).

**B. Adobe Systems Incorporated Cybertip # 74114861.**

64. During the process of investigating MAES, I had submitted a subpoena to PayPal for Gabriel MAES's PayPal account and requested subscriber details, transaction details, and account activity logon history (IP logs) for July 1, 2020, through May 1, 2022. On February 6, 2024, PayPal provided the requested information. I reviewed the transactions records provided by PayPal and discovered that MAES had used his PayPal account to purchase content online from Russian websites and Russian individuals who have been previously identified by law enforcement as suspected of selling CSAM via the Telegram Messenger Application. I identified the following PayPal transactions in which the parties MAES paid to purchase suspected CSAM, identified as Gleb FEIGMAN and Marat Shaigardanov, have been previously identified by U.S. law enforcement as proliferators of CSAM on the Telegram Messenger Application:

- **Date: 18-Jul-2021**  
 Paid: 1434.59 RUB (19.33 USD)  
 Shipped Address Country: Papeete, Tahiti, PF  
 Transaction: Completed  
 Party Paid to: Глеб Файгман (Google Translated Name: Gleb FEIGMAN)  
 Party Acct. No: 1605863402369544927  
 Party Country: Russia  
 Party Email: [chepvicktr@gmail.com](mailto:chepvicktr@gmail.com)  
 Party Tax ID: 20698631300578447
- **Date: 15-May-2021 – 05-Jun-2021**  
 Paid: 70.00 USD  
 Shipped Address Country: Papeete, Tahiti, PF  
 Transaction: Completed – Premium Channel Access  
 Party Paid to: Марат Шайгарданов (Google Translated Name: Marat Shaigardanov)  
 Party Acct. No: 2304119901107178144

Party Country: Russia  
 Party Email: [shbern1@yahoo.com](mailto:shbern1@yahoo.com)  
 Party Tax ID: 20629183543549931

- **Date: 21-Dec-2020 - 11-Jan-2021**
- Paid: 45.0 EUR (55.11 USD)
- Shipped Address Country: Papeete, Tahiti, PF
- Transaction: Completed
- Party Paid to: Марат Шайгарданов (Google Translated Name: Marat Shaigardanov)
- Party Acct. No: 2304119901107178144
- Party Country: Russia
- Party Email: [shbern1@yahoo.com](mailto:shbern1@yahoo.com)
- Party Tax ID: 20469937012921564

65. On March 5, 2024, I conducted a search of the information received from PayPal in DHS and other law enforcement systems and discovered National Center for Missing & Exploited Children (NCMEC) CyberTip Report # 74114861 from Electronic Service Provider (ESP) Adobe Systems Incorporated which reported that, on June 25, 2020, Gabriel MAES, had uploaded three images of suspected CSAM by utilizing Adobe's Revel Lightroom. Adobe Revel was an online media sharing service operated by Adobe Systems and Lightroom was its cloud-based photo service.

66. On or about June 26, 2020, at 16:01:02 hours UTC, the ESP Adobe Systems Incorporated reported to the NCMEC via CyberTip # 74114861, that screen/username: **vahinephoto.com**, identified by Adobe Systems Incorporated as belonging to Gabriel MAES, had uploaded three .JPGs containing depictions of minors engaging in sexually explicit conduct to their account. Adobe Systems Incorporated reported that the upload occurred on the following dates and IP addresses:

- 06/25/2020 at 19:54:37 UTC from IP address 103.4.75.154
- 06/26/2020 at 05:54:29 UTC from IP address 148.66.91.254
- 06/26/2020 at 05:54:34 UTC from IP address 148.66.91.254

67. Adobe Systems Incorporated also reported the suspect account **Screen/User Name: vahinephoto.com** had an associated email addresses of [g.maes@nda.ddec.pf](mailto:g.maes@nda.ddec.pf) (verified) and [tazerty@gmail.com](mailto:tazerty@gmail.com), a phone number 689714770, and address: BP 679 Papeete Tahiti 98713 FR. I know from my training and experience that when a phone number or email address is verified by an ESP, it means that the user indicated that the phone/email belonged to them, the ESP sent a confirmation code or link to the phone/email, and the user correctly and in a timely manner re-entered that code into the ESP's platform or clicked on the link, indicating their dominion and control over that phone/email account.

68. Adobe Systems Incorporated additionally reported the following user activity and associated IP addresses:

- IP Address: 203.185.176.45 (Registration) – 05-11-2013 02:38:00 UTC;
- IP Address: 148.66.90.75 (Login) – 03-30-2020 07:49:00 UTC;
- IP Address: 123.50.106.81 (Login) – 04-17-2020 21:07:00 UTC;
- IP Address: 203.185.173.225 (Login) – 04-29-2020 02:05:00 UTC; and
- IP Address: 103.4.75.161 (Login) – 06-12-2020 04:17:00 UTC;
- IP Address: 148.66.91.196 (Login) – 06-19-2020 03:04:00 UTC.

69. In the CyberTip # 74114861, Adobe Systems Incorporated also reported that the Adobe Product used by the user MAES was Revel Lightroom. Adobe Revel was an online media sharing service operated by Adobe Systems and Lightroom was its cloud-based photo service for amateur photographers to privately save and share photos and videos.

70. Adobe Systems Incorporated also reported the billing information associated with user MAES as following:

- Name: Gabriel MAES;
- Address: La Mennais, BP 679, Papeete Tahiti, France 98713;
- Visa ending in 1082; Expiration Date: 11/2015; and
- American Express Credit Card: Ending in 0529; Expiration Date: 06/2021.

71. Adobe Systems Incorporated additionally submitted that the user account contained approximately 53,263 additional assets that were preserved in anticipation of receiving legal process.

72. On March 5, 2024, I reviewed CyberTip Report # 7411486 and three attached files and describe one of the three files as follows:

a. The video depicts two young prepubescent Caucasian minor females, approximately nine to eleven years of age, due to the small size of their body, childlike facial features, lack of fat or muscle development, very small vaginal structure, lack of hair follicles or pubic hair, lack of breast development, small or underdeveloped shoulders, arms, hands, and hips. Both minor females are completely nude, with one child sitting on a sofa chair with her face, chest, and vagina visible to the camera, while the other child is sitting next to her on the armrest of another sofa chair with her legs spread apart exposing her nude body to the camera, including her face, chest, and vagina. The still image depicts both minor females with long brown hair with scrunchie used to tie their hair in two pigtails. A coloring book and kids coloring magic markers are seen on the glass table in front of the children. One of the minor females can be seen using a color marker to draw on the other child's knee in a playful manner and with a small. The photo is taken by a camera which is positioned either on a tripod or being held by an adult because the camera position is high above both minor females. The focus of the camera lens is framed in a way to intentionally expose the nude bodies of the two minor children without any other distractions.

I have viewed this file and based on my training and experience, I believe the file described above meet the federal definition of child pornography, as defined in 18 U.S.C. 2256(8).

73. For these reasons, I am seeking the below described subscriber account data in order to identify files associated with MAES Adobe Systems Incorporated account that

were possessed by MAES and transported by MAES at the time of his arrest on July 19, 2023, at the Seattle Tacoma International Airport after he arrived on a flight in bound from Paris, France to Seattle on Air Tahiti Nui (TN 57) with the final destination of Tahiti.

#### **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

74. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Adobe Systems Incorporated to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

#### **CONCLUSION**

75. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Adobe Systems Incorporated. Because the warrant will be served on Adobe Systems Incorporated, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

76. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

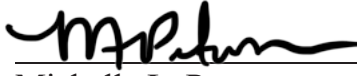
77. The affidavit and application are being presented by reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41(d)(3).

78. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, U.S.C., §

2252(a)(4)(B), (b)(2), Possession of Child Pornography, and Transportation of Child  
Pornography Title 18, U.S.C. 2252(a)(1), (b)(1), has been committed by Gabriel MAES.  
There is also probable cause to search the information described in Attachment A for  
evidence, instrumentalities, contraband, and fruits of these crimes further described in  
Attachment B.

**SHAFQAT M**  
**MIRZA**  
Digitally signed by  
SHAFQAT M MIRZA  
Date: 2024.03.19  
09:55:44 -07'00'  
Shafqat M. Mirza, Affiant  
Special Agent, HSI

The above-named agent provided a sworn statement to the truth of the foregoing  
affidavit by telephone on this 20<sup>th</sup> day of March, 2024.

  
Michelle L. Peterson  
United States Magistrate Judge

**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with Adobe Systems Incorporated  
**Screen/User Name: vahinephoto.com** with associated email addresses of  
[g.maes@nda.ddec.pf](mailto:g.maes@nda.ddec.pf) (verified) and [tazerty@gmail.com](mailto:tazerty@gmail.com), a phone number 689714770, ,  
and address: BP 679 Papeete Tahiti 98713 FR that is stored at premises owned,  
maintained, controlled, or operated by Adobe Systems Incorporated, a company  
headquartered in San Francisco, California.

**ATTACHMENT B****Particular Things to be Seized****I. Information to be disclosed by Adobe Systems Incorporated**

To the extent that the information described in Attachment A, **Screen/User Name:** **vahinephoto.com** with associated email addresses of [g.maes@nda.ddec.pf](mailto:g.maes@nda.ddec.pf) (verified) and [tazerty@gmail.com](mailto:tazerty@gmail.com), a phone number 689714770, , and address: BP 679 Papeete Tahiti 98713 FR is within the possession, custody, or control of Adobe Systems Incorporated, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Adobe Systems Incorporated, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Adobe Systems Incorporated is required to disclose the following information to the government for the user listed in Attachment A for the dates of **June 1, 2020, though July 19, 2023**, UTC<sup>5</sup>:

a. Subscriber basic contact information including subscriber, name, birth date, email address(es), physical address (city, state, zip, country), all telephone numbers, screen name and any associated website;

b. Basic subscriber information (BSI) including Subscriber Identification Number, Date and Time stamp of account creation date displayed in GMT, IP address at account sign-up, Logs in GMT showing source and destination IP addresses and ports; most recent Logins in GMT, registered mobile number(s), verification on whether publicly viewable, and all advertising identification number(s), as well as all devices used to access the account, including IMEI numbers, ICCID numbers, all descriptions of make and model, push-tokens, any additional associated accounts;

c. Customer service records: All subscriber contacts with customer support including notifications or complaints of the account being hacked or stolen, or

---

<sup>5</sup> As detailed herein, June 1, 2020, is the date Adobe Systems Incorporated issued a Cybertip for MAES' account. July 19, 2023, is the date MAES was arrested at Seattle Tacoma International Airport.

1 any other issue with the use of or access to the Adobe account that were created,  
2 uploaded, adjusted, accessed, used, modified, or deleted;

3 d. Subscriber financial account information and account status history;

4 e. Images: All photos, videos, and other depictions associated with the  
5 account, in any format or media. Law enforcement will search these files and only seize  
6 child pornography defined in 18 U.S.C. § 2256, in addition to all depictions which  
7 demonstrate dominion and control over the account;

8 f. Postings, communications, biographical information, or other  
9 information identifying the suspect account user and/or any other persons transmitting  
10 depictions of minors engaged in sexually explicit conduct or evidencing the transmissions  
11 thereof;

12 g. Adobe shall produce all messages and documents related to the  
13 above account. Law enforcement will search these files and only seize child pornography  
14 defined in 18 U.S.C. § 2256, in addition to all depictions which demonstrate dominion  
15 and control over the account (including any attachments thereto), and any profile  
16 information from other file- or photo-sharing websites;

17 h. Device information documenting the devices used by the suspect  
18 account to include information about the suspect account's hardware and software (to  
19 include hardware model, operating system version, device memory, advertising  
20 identifiers, unique application identifiers, apps installed, unique device identifiers,  
21 browser type, language, battery level, and time zone);

22 i. Device information documenting the wireless and mobile network  
23 connections, to include mobile phone number, service provider, IP address, and signal  
24 strength;

25 j. Information collected by cookies and other technologies to include  
26 information when the suspect account interacted with services Adobe offers through one  
27 of its partners, such as advertising and commerce features;

k. Log information such as:

- i. details about how the suspect account used Adobe services;
- ii. device information, such as the suspect account's web browser type and language;
- iii. access times;
- iv. pages viewed;
- v. IP address;
- vi. identifiers associated with cookies or other technologies that may uniquely identify the suspect account's device or browser; and
- vii. pages the suspect account visited before or after navigating to Adobe's website.

Adobe Systems Incorporated is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant.

## **II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Title 18, U.S.C., § 2252(a)(4)(B), (b)(2), Possession of Child Pornography, and Transportation of Child Pornography Title 18, U.S.C. 2252(a)(1), (b)(1), since the creation of the account, including, for the user identified on Attachment A, information pertaining to the following matters:

- a. Evidence identifying the person(s) exercising dominion and control over the suspect account;
- b. Financial account information and account status history;
- c. Evidence indicating the receipt, distribution, or transportation of sexually explicit material depicting minors;
- d. All photos, videos, and other depictions associated with the account that depict child pornography defined in 18 U.S.C. § 2256;

1  
2 e. Images associated with the account belonging to the Adobe Systems  
3 Incorporated suspect account user;

4 f. Postings, communications, biographical information, or other  
5 information identifying the suspect account user and/or any other persons transmitting  
6 depictions of minors engaged in sexually explicit conduct, and attempts thereof, or  
7 evidencing the transmissions thereof;

8 g. Evidence indicating how and when the Adobe Systems Incorporated  
9 account was accessed or used, to determine the chronological and geographic context of  
10 account access, use, and events relating to the crime under investigation and to the Adobe  
11 account owner;

12 h. Information about the content created or provided by the suspect  
13 account, when the content was viewed and the metadata that is provided with the content;

14 i. Data related to linked services;

15 j. User attribution evidence identifying the account user's devices,  
16 software, sensors, operating version, advertising identifiers, installed applications, unique  
17 identifiers, browser data, time zone, wireless and mobile network connections to include  
18 numbers, providers, IP addresses, and data related thereto;

19 k. Evidence of the Adobe account user's state of mind as it relates to  
20 the crimes under investigation;

21 l. The identity of the person(s) who created or used the user ID,  
22 including records that help reveal the whereabouts of such person(s), and to establish  
23 dominion and control over the account during this time period.

24 This warrant authorizes a review of electronically stored information, communications,  
25 other records and information disclosed pursuant to this warrant in order to locate  
26 evidence, fruits, and instrumentalities described in this warrant. The review of this  
27 electronic data may be conducted by any government personnel assisting in the  
investigation, who may include, in addition to law enforcement officers and agents,

1 attorneys for the government, attorney support staff, and technical experts. Pursuant to  
2 this warrant, HSI may deliver a complete copy of the disclosed electronic data to the  
3 custody and control of attorneys for the government and their support staff for their  
4 independent review.  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27